a switch scenario, the ARP packets will need to be addressed to the target host, not to a gateway. To achieve this with subnet aware hosts, they must be configured to be their own default gateway. If the switch has not learned the MAC address of the target, then it will forward the ARP request to the appropriate subnet. If the switch has learned the target MAC address then it will reply for the target host with the target host's MAC address. If the switch knows that the target is on the same port that it received the ARP request on, it will not respond. It will instead drop the packet and let the host respond. In either case, the unicast packets that follow will be sent to the destination MAC address of the host, not the switch. This in turn will allow all the unicast traffic to be sent via level 2 switching, although the switches do not route unicast packets, they do route the broadcast packets and for this reason they need to learn the network topology as a router would. To do this they can be either manually configured with all of the subnets (the IP subnet will be the VLAN broadcast domain) or they can run some type of routing protocol such as a modified RIP.

Detailed Description Text - DETX (96):

Turning to FIG. 5, the next two scenarios will use a single switch. In these scenarios the switch 506 has been configured with 2 VLANs with ports 1 and 2 in VLAN 1 and port 3, 4 and 5 in VLAN 2. The VLANs are defined based on the IP subnet that they connect to, VLAN 1 is associated with IP subnet 10.1.8.x and VLAN 2 is associated with IP subnet 10.2.8.x.

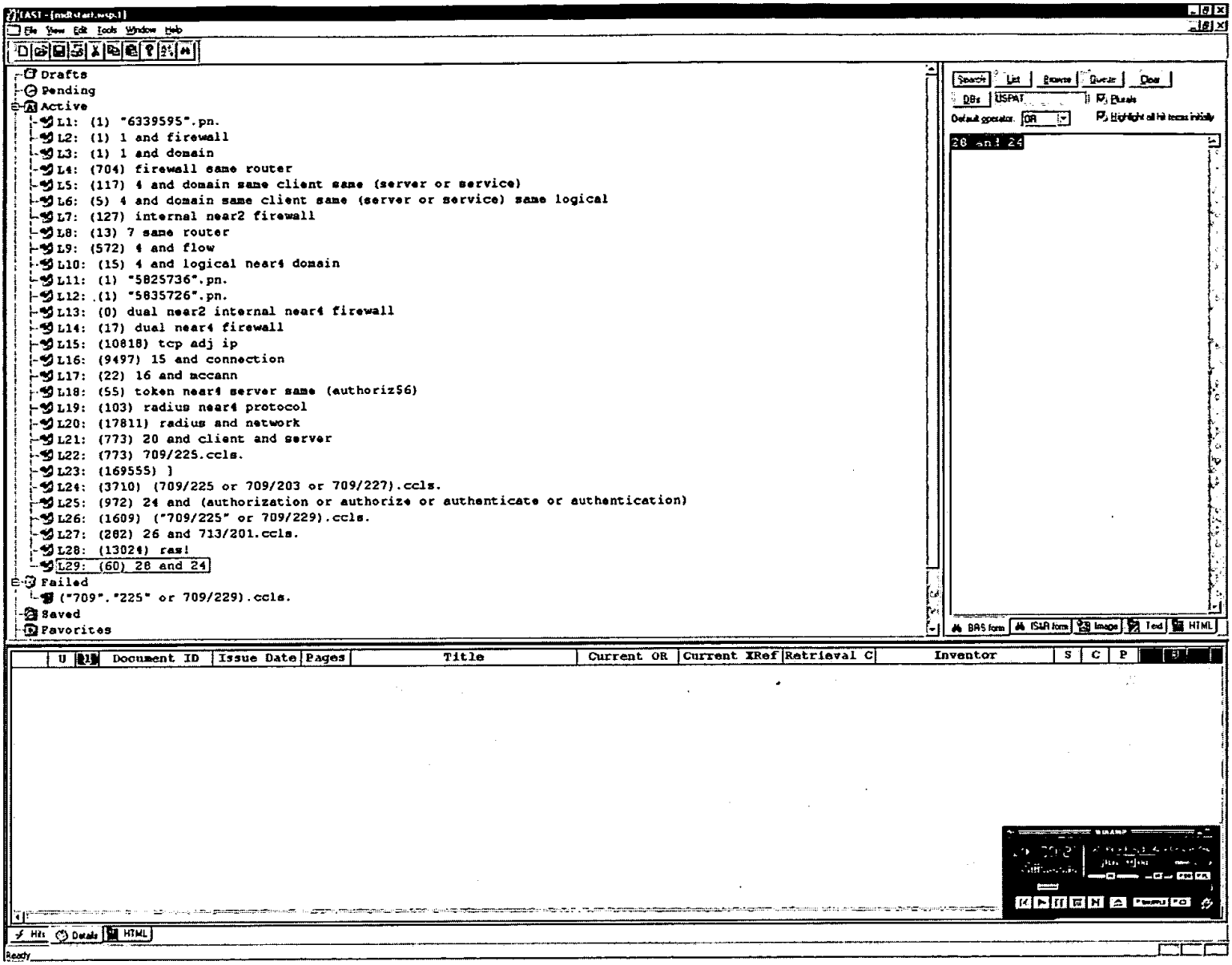
Detailed Description Text - DETX (98):

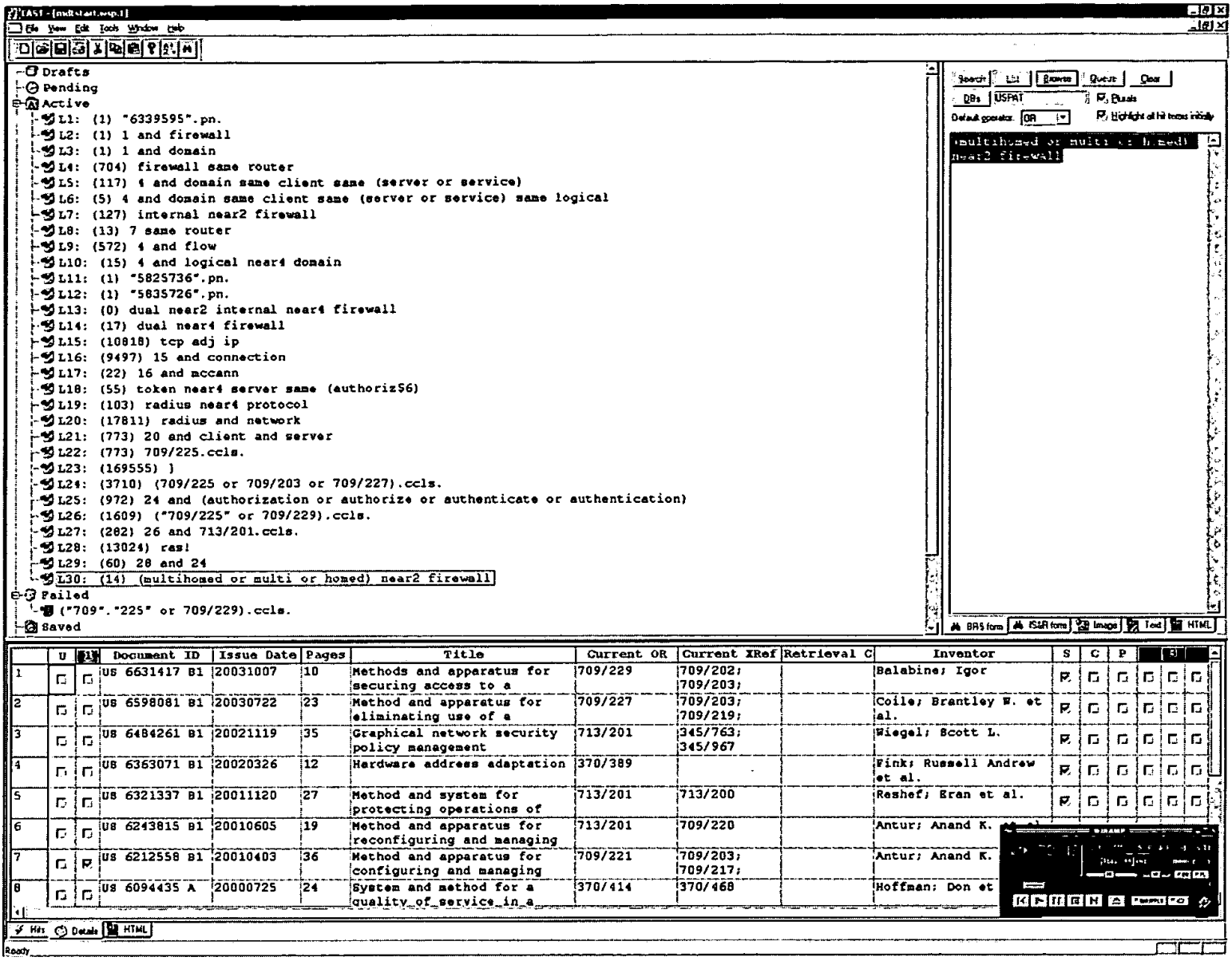
In this scenario, the hosts and switch have just been booted and no ARP caches or MAC address tables exist in any of the network components. Host A 501 wishes to talk to HOST C 503. Host A 501 will send an ARP to find the MAC address of HOST C 503 (10.2.8.1). The source MAC address in the ARP request will be Host A's 501 MAC address and the destination MAC address will be a broadcast address. The switch 406 receives this packet and learns that HOST A 501 is on port 1 and sends the packet to the VSE because the destination is a broadcast. The VSE analyzes the packet and because the destination is the 10.2.8.x network the VSE forwards the ARP request packet out on ports 3, 4 and 5. The VSE also adds HOST A 501 to its ARP cache and marks the ASIC's MAC address table to indicate that future unicast traffic from HOST A 501 is not to be sent to the VSE if the destination MAC address is known. HOST C 503 will receive the ARP broadcast and send a unicast ARP reply. When the switch 406 receives the reply it adds HOST C 503 to the MAC address table and although the destination MAC address is known, this is the first time that the source MAC address of HOST C 503 has been heard from and the unicast packet is sent to the VSE. The VSE analyzes the packet and adds Host C 503 to its ARP cache and marks the ASIC's MAC address table to indicate that future unicast traffic from HOST C 503 is not to be sent to the VSE if the destination MAC address is known. The switch 406 then forwards the ARP reply to port 1 so HOST A 501 can add HOST C 503 to its ARP cache. At this point, all future unicast traffic sent between HOST A 501 and C 503 is switched at level 2 and bypasses the VSE. Whether packets are sent on the same VLAN or to a different VLAN, the broadcasts always go to the VSE. The VSE then decides which ports to send the packet out on. The only difference is when a packet is destined for the same VLAN, the broadcast would not be sent to all ports in the VLAN--the originating port would be left out.

Detailed Description Text - DETX (100):

This scenario starts with the assumption that scenario 1 above has just run (i.e. the switch 506 has HOST A 501 and C 503 in MAC address and ARP caches). Host B 502 now wishes to talk to HOST C 503. Host B 502 sends an ARP to HOST C 503. The source MAC address in the ARP request will be Host B's 502 MAC address and the destination MAC address will be a broadcast address. The switch 506 receives this packet and learns that HOST B 502 is on port 2 and sends the packet to the VSE because the destination is a broadcast. The VSE analyzes the packet and because the destination is 10.2.8.1 is in its ARP cache

	Document ID	Pag	Current	Current XR	S	S2	PT
1	US 6339595	61	370/392	370/400;	☑	☑	☐
2	US 6101188	20	370/401	370/255;	☑	☐	☐
3	US 5963939	118	707/4	345/700;	☑	☐	☐
4	US 5926463	31	370/254	370/410;	☑	☐	☐
5	US 5920699	29	709/225		☑	☐	☐
6	US 5905723	7	370/351	340/2.27;	☐	☐	☐
7	US 5734865	29	709/250	370/254	☐	☐	☐
8	US 5636371	28	703/26	340/825.52	☐	☐	☐
9	US 5337311	10	370/403	370/452;	☐	☐	☐


File View Edit Tools Window Help
Drafts
Pending
Active
L1: (1) "6339595".pn.
L2: (1) 1 and firewall
L3: (1) 1 and domain
L4: (704) firewall same router
L5: (117) 4 and domain same client same (server or service)
L6: (5) 4 and domain same client same (server or service) same logical
L7: (127) internal near2 firewall
L8: (13) 7 same router
L9: (572) 4 and flow
L10: (15) 4 and logical near4 domain
L11: (1) "5825736".pn.
L12: (1) "5835726".pn.
L13: (0) dual near2 internal near4 firewall
L14: (17) dual near4 firewall
L15: (10818) tcp adj ip
L16: (9497) 15 and connection
L17: (22) 16 and mccann
L18: (55) token near4 server same (authoriz56)
L19: (103) radius near4 protocol
L20: (17811) radius and network
L21: (773) 20 and client and server
L22: (773) 709/225.ccls.
L23: (169555))
L24: (3710) (709/225 or 709/203 or 709/227).ccls.
L25: (972) 24 and (authorization or authorize or authenticate or authentication)
L26: (1609) ("709/225" or 709/229).ccls.
L27: (282) 26 and 713/201.ccls.
L28: (13024) ras!
L29: (60) 28 and 24
Failed
("709"."225" or 709/229).ccls.
Saved
Favorites
Search
List
Browse
Queue
Clear
DBs
USPAT
Plurals
Default operator:
OR
Highlight all hit terms initially
28 and 24
BRS form
ISR form
Image
Text
HTML
U
Document ID
Issue Date
Pages
Title
Current OR
Current XRef
Retrieval C
Inventor
S
C
P
Hits
Details
HTML
Ready



	U		Document ID	Issue Date	Pages	Title	Current OR	Current XRef	Retrieval C	Inventor	S	C	P
1	☐	☐	US 6631417 B1	20031007	10	Methods and apparatus for securing access to a	709/229	709/202; 709/203;		Balabine; Igor	☑	☐	☐
2	☐	☐	US 6598081 B1	20030722	23	Method and apparatus for eliminating use of a	709/227	709/203; 709/219;		Coile; Brantley W. et al.	☑	☐	☐
3	☐	☐	US 6484261 B1	20021119	35	Graphical network security policy management	713/201	345/763; 345/967		Wiegel; Scott L.	☑	☐	☐
4	☐	☐	US 6363071 B1	20020326	12	Hardware address adaptation	370/389			Fink; Russell Andrew et al.	☑	☐	☐
5	☐	☐	US 6321337 B1	20011120	27	Method and system for protecting operations of	713/201	713/200		Reshef; Eran et al.	☑	☐	☐
6	☐	☐	US 6243815 B1	20010605	19	Method and apparatus for reconfiguring and managing	713/201	709/220		Antur; Anand K.	☑	☐	☐
7	☐	☑	US 6212558 B1	20010403	36	Method and apparatus for configuring and managing	709/221	709/203; 709/217;		Antur; Anand K.	☑	☐	☐
8	☐	☐	US 6094435 A	20000725	24	System and method for a quality of service in a	370/414	370/468		Hoffman; Don et	☑	☐	☐

Hits
Details
HTML
Ready